



Department of Homeland Security Daily Open Source Infrastructure Report for 22 June 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The U.S. Energy Information Administration reports that non-Organization of the Petroleum Exporting Countries crude oil producers such as Russia and Canada will provide about two-thirds of the world's oil demand growth through 2030. (See item [2](#))
- Newsday reports investigators have found fire hazards so significant that they could cause an explosion or allow dangerous natural gas to be drawn into the terminal in the new Southwest Airlines terminal at MacArthur Airport in Ronkonkoma, New York. (See item [13](#))
- The Organization for the Advancement of Structured Information Standards has approved the Emergency Data Exchange Language Distribution Element as a data-sharing standard that provides role-based information sharing for emergency responders in a crisis. (See item [32](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *June 21, Associated Press* — **Simulators train future coal miners about underground dangers.** The mine simulators at Hazard Community and Technical College in eastern Kentucky give students interested in a career in mining a taste of underground dangers without risking their lives. After the disasters this year at the Sago mine in West Virginia and the Darby

mine in Kentucky, experts say the new technology is a way to improve training for miners. Three-dimensional mine simulators have gained popularity within the coal industry and are being used in different forms from Appalachia to Australia. The U.S. Mine Safety and Health Administration uses a simulation lab at its academy in Beckley, WV, which creates smoky or gaseous conditions for students practicing rescue techniques. Industry experts see the simulators as a way to attract more people into mines as roughly 50 percent of the current mine work force prepares to retire within the next decade. Instructors can challenge the future miners by simulating machine failure, poor visibility conditions, gas leaks, and other emergencies. The simulators measure a student's performance by recording all his actions and any operating errors.

Source: http://www.mercurynews.com/mld/mercurynews/news/breaking_news/14843538.htm

2. *June 20, Reuters* — **EIA: Non-OPEC fills majority of oil demand growth.**

Non-Organization of the Petroleum Exporting Countries (OPEC) crude oil producers like Russia and Canada will fill about two-thirds of the world's oil demand growth through 2030, the U.S. Energy Information Administration (EIA) said on Tuesday, June 20. Oil producers will pump about 38 million barrels per day (bpd) more in 2030 than they did in 2003 to meet growing demand, the EIA said in its yearly international energy outlook. Global oil consumption will rise to 118 million bpd in 2030 from 80.1 million bpd in 2003, the EIA said. OPEC members will send a larger amount of their oil exports to non-industrialized nations, especially in Asia, the EIA said. In 2030 OPEC shipments to industrialized nations will be nine percentage points lower than 2003, and industrialized countries' share of Middle East OPEC exports will be down 13 percent.

Full report: <http://www.eia.doe.gov/oiaf/ieo/index.html>

Source: <http://www.signonsandiego.com/news/business/20060620-0600-energy-eia-ope.html>

3. *June 19, Government Accountability Office* — **GAO-06-888T: Nuclear Regulatory Commission: Preliminary Observations on Its Process to Oversee the Safe Operation of Nuclear Power Plants (Testimony).** Prior to 2000, the Nuclear Regulatory Commission (NRC) was criticized for having a safety oversight process that was not always focused on the most important safety issues and in some cases, was overly subjective. To address these and other concerns, NRC implemented a new oversight process—the Reactor Oversight Process (ROP). NRC continues to modify the ROP to incorporate feedback from stakeholders and in response to other external events. This testimony by the Government Accountability Office (GAO) summarizes information on how NRC oversees nuclear power plants, the results of the ROP over the past several years, and the aspects of the ROP that need improvement and the status of NRC's efforts to improve them. This testimony discusses preliminary results of GAO's work. GAO will report in full at a later date. GAO analyzed program-wide information, inspection results covering five years of ROP operations, and detailed findings from a sample of 11 plants.

Highlights: <http://www.gao.gov/highlights/d06888thigh.pdf>

Source: <http://www.gao.gov/docsearch/repanetest.html>

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

4. *June 21, Government Accountability Office* — **GAO-06-899T: Homeland Security: DHS Is Addressing Security at Chemical Facilities, but Additional Authority Is Needed (Testimony)**. Terrorist attacks on U.S. chemical facilities could damage public health and the economy. The Department of Homeland Security (DHS) coordinates federal efforts to protect these facilities from attacks. The Government Accountability Office (GAO) was asked to provide a statement for the record based on its report, Homeland Security: DHS Is Taking Steps to Enhance Security at Chemical Facilities, but Additional Authority Is Needed (GAO-06-150, January 27, 2006). GAO reviewed (1) DHS' actions to develop a strategy to protect chemical plants, assist with the industry's security efforts, and coordinate with other federal agencies, (2) industry security initiatives, (3) DHS' authorities and the need for additional security legislation, and (4) stakeholders' views on any requirements to use safer technologies. GAO's report recommended that (1) the Congress consider giving DHS the authority to require the chemical industry to address plant security, (2) DHS complete its Chemical Sector-Specific Plan in a timely manner, and (3) DHS study, with the Environmental Protection Agency (EPA), the security benefits of using safer technologies. DHS agreed in substance with GAO's first two recommendations but expressed concerns about studying safer technologies. GAO continues to see merit in such a study. EPA had no comments.
Highlights: <http://www.gao.gov/highlights/d06899thigh.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-899T>
5. *June 20, KHOU (TX)* — **Texas plant fire puts 2,000 homes in shelter-in-place**. Plastic resin was on fire Tuesday night, June 20, at the Arkama Chemicals in Crosby, TX, prompting a shelter-in-place order for 2,000 Harris County residents as a precaution. The shelter-in-place was cancelled at about 8 p.m. CDT, when the fire was brought under control
Source: http://www.khou.com/news/local/houstonmetro/stories/khou060620_cd_arkamaplant10.a73a6c38.html
6. *June 19, WSOC-TV (NC)* — **Gas line fire destroys several apartments**. A massive fire in Charlotte, NC, Monday, June 19, started after a crew working with a back hoe hit a gas line, which caught fire. The fire spread to nearby trees and the Runway Bay Apartments. Tenants of 12 units were displaced by the fire. After the fire was doused, it was determined the back hoe split an electrical line that sparked the fire and the gas line fueled the flames.
Source: <http://www.wsocv.com/news/9390826/detail.html>

[[Return to top](#)]

Defense Industrial Base Sector

7. *June 20, Defense News* — **Air Force, National Reconnaissance Office reinforce ties**. The leading National Reconnaissance Office (NRO) and U.S. Air Force space program officials divulged details Tuesday, June 20, of development, acquisition and operations agreements meant to better sew the seams binding the service and the agency. The Air Force and NRO also will be working more closely with U.S. Strategic Command to better protect the country's satellites from jamming or other attacks, which U.S. space leaders have identified as a major concern over the past couple of years. The Air Force and NRO agreed to pursue a test program to integrate satellite operations, but not the tasking of spacecraft payloads. NRO Director

Donald Kerr said his next major concern for the space community would be “pursuing space radar.” He also said the NRO would continue to bank heavily on research and development. Lt. Gen. Frank Klotz, Air Force Space Command vice commander, stated the Air Force plans to test and develop smaller, lighter satellites, to make them more operationally responsive for combatant commanders.

Source: <http://www.defensenews.com/story.php?F=1883659&C=america>

8. *June 20, Government Accountability Office* — **GAO-06-455R: Tactical Aircraft: Department of Defense Should Present a New F-22A Business Case before Making Further Investments (Correspondence).** The F-22A is the Air Force’s next generation air superiority fighter aircraft. In March 2005, the Government Accountability Office (GAO) reported that despite substantial changes to the F-22A program since it started in 1986, Air Force leaders have not developed a new business case for investing billions more dollars to modernize the aircraft. Over time quantities have been reduced, and in recent years both funding and quantities have been in a state of flux. Given significant changes in quantities and planned capabilities, the large investments still planned, and the potential for further changes, GAO was requested to review the F-22A program. Specifically, GAO assessed the need for a new business case before further investments are made in the F-22A program and statutory criteria the Air Force is required to meet to enter a multi-year contract for the remaining aircraft.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-455R>

9. *June 19, Government Computer News* — **Department of Defense, military take hands-on approach to Quadrennial Defense Review.** The writers of the Quadrennial Defense Review are now shifting gears to become executors of the guidance. Senior Defense and service officials will soon be running experiments, examining how systems are governed, managed and implemented under four categories which make up the Joint Capabilities Portfolio. Those categories are joint command and control, joint network-centric operations, joint logistics and battle space awareness. Within each of the categories of the Joint Capabilities Portfolio, military leaders will be looking for systems to be developed so information can be shared across military organizations.

Source: http://www.gcn.com/online/vol1_no1/41091-1.html

[\[Return to top\]](#)

Banking and Finance Sector

10. *June 20, Government Technology* — **Information Policy Institute examines data breach notification legislation.** A recent examination of data breach notification conducted by the Information Policy Institute identifies some pitfalls in many proposed data breach notification bills and laws. The study, *Towards a Rational Personal Data Breach Notification Regime*, examines trends in identity theft, identity fraud, and data breaches and proposes elements for an effective notification system. The study finds: identity theft and fraud have not been growing; the damage done has been declining; responses by industry are having a positive impact in preventing identity crimes and reducing the damage done. How and when consumers are notified matters a great deal for minimizing damage. If consumers are "over-notified" they will pay less attention and fail to direct their efforts to incidences where monitoring is crucial. The

study points out that how the breach that prompts notification is defined is crucial in avoiding "over-notification" where consumers are inundated with information. Uniformity in the notification requirement also matters.

Source: <http://www.govtech.net/magazine/story.php?id=99946>

11. *June 20, Associated Press* — **French police detain 17 people in probe of suspected radical Islamic terror financing.** Police have detained a prayer leader at a suburban Paris mosque and 16 associates as part of an investigation into alleged terror financing, a police official said Tuesday, June 20. Dahou Meskine, imam at the mosque in the suburb of Clichy-sous-Bois, and the 16 others were apprehended in separate raids around the capital early Monday. Prosecutors believe the suspects were involved in a money-laundering scheme to benefit radical Islamic groups. The arrests were part of a probe launched 18 months ago based on information from Tracfin, an agency within the Finance Ministry that tracks money laundering. French intelligence officials say terror cells here have been changing their financing and planning methods, with funds often coming through inventive, small-scale sources such as halal butcher shops, trade in cannabis, and ATM scams.

Source: <http://www.tkb.org/NewsStory.jsp?storyID=126433>

12. *June 20, Associated Press* — **Ohio University suspends two over data theft.** Ohio University said Tuesday, June 20, it has suspended two information technology supervisors over recent breaches by hackers who may have stolen 173,000 Social Security numbers from school computers. The two were suspended pending the school's investigation of the breaches, five of which have happened since March 2005. Citing results from an independent audit, the school also said University President Roderick McDavis will ask trustees for up to \$2 million to improve computer security. The school said in April it had discovered a computer breach at its training center for fledgling businesses. Since then, electronic break-ins also were reported at the school's alumni office, health center, and the department that handles records for businesses the university hires. About two dozen people have told the school they were victimized by identity theft in the past year.

More information on the Ohio University data theft: <http://www.ohio.edu/datatheft>

Source: <http://abcnews.go.com/Technology/wireStory?id=2100553>

[[Return to top](#)]

Transportation and Border Security Sector

13. *June 21, Newsday (NY)* — **Problems at MacArthur Airport.** Investigators have found serious fire hazards in the new Southwest Airlines terminal at MacArthur Airport in Ronkonkoma, NY. The hazards are so significant that they could cause an explosion or allow dangerous natural gas to be drawn into the terminal, Suffolk County District Attorney Thomas Spota said. In an interview on Tuesday, June 20, Spota said sprinklers, rather than a chemical fire-suppression system, had been installed in the terminal's main electrical control room, which controls all power in the building. That is a problem because water could cause electricity to arc, sparking an explosion, Spota said. Islip Town Attorney Pierce Cohalan said on Tuesday that the town was aware of problems in the terminal. Outside the Southwest terminal, natural gas pipes are located right underneath air conditioning intake manifolds, according to a former town employee. If there were a gas leak, natural gas could get pulled into the new terminal's main

ventilation system. Southwest spokesperson Whitney Eichinger said in a statement that the airline would conduct its own review of the problems.

Source: <http://www.newsday.com/news/local/longisland/ny-liair21.0.3414930.story?coll=ny-homepage-bigpix2005>

14. *June 21, Associated Press* — **AirTran flights delayed due to glitch.** AirTran Airways passengers experienced sporadic delays in boarding flights Tuesday, June 20, because a new computer system at the airline was not working properly. The Orlando, FL–based airline, which has its hub in Atlanta, said it has had problems processing passengers for more than 15 hours after the new system went online at 4 a.m. EDT, resulting in long lines at many airports that it serves. The biggest problems were at Hartsfield–Jackson Atlanta International Airport, where the airline usually handles 250 flights a day, spokesperson Judy Graham–Weaver said. The airline was encouraging passengers to print out their boarding passes online, or show up for their flights two to three hours early. AirTran was investigating what caused the computer problem, Graham–Weaver said.

Source: http://biz.yahoo.com/ap/060620/airtran_computer_glitch.html?.v=2

15. *June 21, Associated Press* — **PBGC gets Delta pilots pension notice.** The government's pension insurer, Pension Benefit Guaranty Corp (PBGC) said Tuesday, June 20, it has received Delta Air Lines Inc.'s notice of its intention to terminate its pilots' pension plan. Once the pilots' pension is terminated, the PBGC will be responsible for paying out benefits to the 6,000 pilots, who will receive a reduced amount compared to what they were entitled under the airline's pension plan. The notice to the PBGC listed 13,284 fully vested active pilot participants and retirees or beneficiaries currently receiving benefits. Delta is seeking to terminate the pilot plan effective September 2. A bankruptcy court judge would have to approve the request. The airline still hopes to save its other employees' pension plans. Atlanta–based Delta filed for bankruptcy protection last September.

Source: http://biz.yahoo.com/ap/060620/delta_pilots.html?.v=2

16. *June 21, Associated Press* — **Power problems halt trains in New York, New Jersey.** Power problems temporarily halted train service between New York City and New Jersey during the Wednesday morning rush, June 21, causing delays along the Northeast Corridor, New Jersey Transit said. A notice on the system's Website blamed the delays on "Amtrak power problems" but offered no other details. Cliff Black, an Amtrak spokesperson, said sometime between 7:30 a.m. and 8:30 a.m. EDT there was a brief power fluctuation in the New York area.

Source: http://www.boston.com/news/nation/articles/2006/06/21/power_problems_halt_trains_in_ny_nj/

17. *June 21, Government Accountability Office* — **GAO–06–653T: Air Traffic Control Modernization: Status of the Current Program and Planning for the Next Generation Air Transportation System (Testimony).** The Federal Aviation Administration's (FAA) effort to modernize the nation's air traffic control (ATC) system has been listed by GAO as a high risk program for more than a decade now, due to systemic management and acquisition problems. Two relatively new organizations housed within FAA—the Air Traffic Organization (ATO) and the Joint Planning and Development Office (JPDO)—have been given the bulk of the responsibility for planning and implementing these modernization efforts. Congress created ATO to be a performance–based organization that would improve the culture, structure, and

processes and improve accountability in the ATC modernization program. Congress created JPDO, made up of seven partner agencies, to coordinate the federal and nonfederal stakeholders necessary to plan a transition from the current air transportation system to the “next generation air transportation system” (NGATS). This testimony is based on the Government Accountability Office’s (GAO) recently completed and ongoing studies of the ATC modernization program. GAO provides information on (1) the status of ATO’s efforts to implement processes and other initiatives aimed at efficiently managing and modernizing the current ATC system and (2) the status of JPDO’s planning efforts and the key challenges that JPDO faces in planning for NGATS.

Highlights: <http://www.gao.gov/highlights/d06653thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-653T>

18. *June 21, Government Accountability Office* — **GAO-06-898T: Freight Railroads:**

Preliminary Observations on Rates, Competition, and Capacity Issues (Testimony). The Staggers Rail Act of 1980 largely deregulated the freight railroad industry, giving the railroads freedom to price their services according to market conditions and encouraging greater reliance on competition to set rates. The act recognized the need for railroads to use demand-based differential pricing in the deregulated environment and to recover costs by setting higher rates for shippers with fewer transportation alternatives. The act also recognized that some shippers might not have access to competitive alternatives and might be subject to unreasonably high rates. It established a threshold for rate relief and granted the Interstate Commerce Commission and the Surface Transportation Board (STB) the authority to develop a rate relief process for those “captive” shippers. This testimony provides preliminary results on the Government Accountability Office’s (GAO) ongoing work and addresses (1) the changes that have occurred in the freight railroad industry since the enactment of the Staggers Rail Act, including changes in rail rates and competition in the industry, (2) the alternative approaches that have been proposed and could be considered to address remaining competition and captivity concerns, and (3) the projections for freight traffic demand over the next 15 to 25 years, the freight railroad industry’s projected ability to meet that demand, and potential federal policy responses. To fulfill these objectives, GAO examined STB data, interviewed affected parties, and held an expert panel.

Highlights: <http://www.gao.gov/highlights/d06898thigh.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-898T>

[\[Return to top\]](#)

Postal and Shipping Sector

- 19. *June 21, WQOW (WI)* — **Wisconsin post office drill.**** The Eau Claire, WI, main post office held a biohazard drill on Tuesday, June 20. The facility has an anthrax detection machine, and the drill focused on what would happen if the machine’s alarm went off. The drill involved local fire and police departments along with postal inspectors from Minnesota.

Source: http://www.wqow.com/news/articles/article_6970.shtml

[\[Return to top\]](#)

Agriculture Sector

20. *June 21, Stop Soybean Rust News* — **New Website looks at yield loss, Brazil data on soybean rust.** A new Website for an international soybean–rust yield loss study offers a look at a preliminary yield–loss calculator, as well as unique information resources from Brazil. The project, the "Yield Loss Prediction Tool for Field–Specific Risk Management of Asian Soybean Rust," is headed by Saratha Kumudini, a plant physiologist in the University of Kentucky Department of Plant and Soil Sciences. The objective of the current study is to predict yield loss from soybean rust damage at various reproductive stages of development. The ultimate aim of this international study is to develop an interactive software tool that would determine the farmer's current yield potential and the yield loss predicted if soybean rust should defoliate the crop. The potential yield loss could be weighed against the cost of the fungicide application to make sound management decisions.
Project Website: <http://www.uky.edu/Ag/Agronomy/Department/sbr>
Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=857>
21. *June 20, Fort Morgan Times (CO)* — **Emergency grazing approved.** In continuing response to drought in Colorado, the U.S. department of Agriculture's Farm Service Agency (FSA) announced Monday, June 19, the authorization of emergency grazing on Conservation Reserve Program (CRP) acreage in Morgan County until August 1. Emergency haying is authorized to be implemented beginning July 16. Approval for emergency grazing in the county will provide forage for livestock and help producers in areas most severely impacted by the drought conditions.
Source: <http://www.fortmorgantimes.com/Stories/0,1413,164~8305~33344 08,00.html>
22. *June 18, Herald News (IL)* — **Asian carp killed.** Thousands of Asian carp have died in the Illinois River on a 110–mile stretch ranging from Starved Rock State Park in Utica to Havana. A biologist with the Illinois Department of Natural Resources made the discovery when he went to the river to collect live carp for a spawning study. He reportedly found numerous carcasses weighing about 50 pounds apiece. Bacterial infection has been ruled out.
Source: http://www.suburbanchicagonews.com/heraldnews/city/4_1_1 JO1 8 FISH S2.htm
23. *June 08, Columbian (WA)* — **Botulism outbreak kills chinook at hatchery.** Nearly all the 3.5 million fall chinook salmon smolts scheduled for release from Ringold Springs Hatchery on the upper Columbia River have died, probably due to botulism poisoning. The Washington Department of Fish and Wildlife said the five–month–old fish represent about 20 percent of the fall chinook salmon smolts for release from the upper Columbia. The vast majority of fall chinook in the upper Columbia River are wild fish, originating from the Hanford Reach, the free–flowing stretch downstream of Priest Rapids Dam. John Kerwin, hatcheries division manager, said the three–inch smolts began dying shortly after they were transported in mid–May from Oregon's Bonneville Hatchery to Ringold. Tests for routine viruses and bacterial infections came back negative. There were no problems at Bonneville Hatchery, which rears the fish under an agreement with the U.S. Fish and Wildlife Service and U.S. Army Corps of Engineers. Washington officials learned two of 10 samples sent to Cornell University tested positive for the bacteria that produce botulism.
Source: http://www.redorbit.com/news/science/532470/botulism_outbreak_kills_fall_chinook_at_ringold_springs_hatchery/index.html?source=r_science

Food Sector

- 24. *June 21, U.S. Food and Drug Administration* — Guidance issued to prevent inadvertent introduction of allergens or toxins into the food and feed supply.** The U.S. Food and Drug Administration (FDA) Wednesday, June 21, issued guidance to industry to help prevent the inadvertent introduction of allergens or toxins into the U.S. food and feed supply. The guidance provides greater transparency by explaining how the agency will conduct its early safety evaluation of new proteins in new plant varieties, including bioengineered varieties, that are in development for possible use as food for humans or animals. This guidance is focused on resolving any potential food safety issues prior to possible inadvertent introduction of material from a new plant variety for which FDA has not been consulted. Under the guidance, entitled "Guidance for Industry: Recommendations for the Early Food Safety Evaluation of New Non-Pesticidal Proteins Produced by New Plant Varieties Intended for Food Use," developers would voluntarily provide FDA with information about the food safety of new proteins at a relatively early stage of development of the new crops. Following a decision to commercialize a particular crop, it is recommended that each developer participate in FDA's voluntary premarket consultation procedures.
Guidance document: <http://www.cfsan.fda.gov/~dms/guidance.html>.
Source: <http://www.fda.gov/bbs/topics/NEWS/2006/NEW01393.html>

- 25. *June 21, New York Times* — Japan to resume imports of beef from the U.S.** Japan said it would resume imports of U.S. beef after reaching an agreement that allows Japanese inspectors into U.S. meatpacking plants. Japan was the largest foreign market for U.S. cattle ranchers before December 2003, when it was closed to them after a lone case of mad-cow disease was found in Washington state. Japan imported \$1.4 billion worth of American beef in 2003 before the ban was imposed. Japan first agreed to resume imports in December 2005, only to block them again a few weeks later when backbone parts were found in a shipment from a Brooklyn, NY, meatpacker. Spinal chords, brains and the surrounding body parts remained banned under the December 2005 agreement because they are the parts most likely to carry the disease. The new agreement reached Wednesday, June 21, calls for Japan to resume beef imports from the U.S. on the condition that Japanese officials be allowed to monitor American compliance, a spokesperson for Japan's agriculture ministry said. He said the agreement allows Japanese health and agricultural officials to directly inspect meatpacking plants in the U.S., and to accompany American officials on their spot inspections.
Source: http://www.nytimes.com/2006/06/21/business/worldbusiness/21cnd-beef.html?_r=1&oref=slogin

Water Sector

- 26. *June 20, Pennsylvania Department of Environmental Protection* — Treatment plant spills sewage.** Pennsylvania Department of Environmental Protection Regional Director Joseph Feola

Tuesday, June 20, announced that a Monday, June 19, power outage at the Ambler Borough wastewater treatment plant resulted in the release of approximately 55,000 gallons of raw sewage into the Wissahickon Creek, a stream impacted less than a week ago by problems discovered at the Upper Gwynedd wastewater treatment plant. Permanent power was restored early Tuesday, June 20, and the plant is operating within normal limits using ultraviolet light disinfection. The ongoing investigation of a fish kill that occurred upstream last week near the outfall of the Upper Gwynedd wastewater treatment plant continues.

Source: <http://www.depweb.state.pa.us/news/cwp/view.asp?Q=508175&A=3>

[[Return to top](#)]

Public Health Sector

27. *June 21, Agence France–Presse* — Children vaccinated against polio in Bangladesh. More than 21 million Bangladeshi children under the age of five have been vaccinated against polio. Some 600,000 volunteers took part in the program after a new case was identified in January. The country of 140 million people had previously not seen any polio cases since August 2000. The vaccination campaign, carried out on three separate days in April, May and June, reached 96 percent of the country's 22 million under-fives, said the United Nations Children's Fund country representative Louis-Georges Arsenault Wednesday, June 21.

Global Polio Eradication Initiative: <http://www.polioeradication.org/>

Source: http://news.yahoo.com/s/afp/20060621/hl_afp/bangladeshhealthpolio_060621120410: ylt=AuPPK9Wrao1bxj1XgUYn_T2JOrgF: ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--

28. *June 21, Bloomberg* — Indonesia, World Health Organization discuss bird flu control plan. Indonesian officials began a meeting with world health authorities Wednesday, June 21, to help fight bird flu, which has killed a person every six days in the nation this year. Keiji Fukuda, the coordinator of the World Health Organization's global influenza program, and other experts will advise the government on ways to gain better control of the H5N1 flu strain that's spread in poultry to most of the country's 33 provinces. The Southeast Asian nation accounts for a third of the 130 human H5N1 fatalities reported worldwide since late 2003. Indonesia's strategy of using animal vaccines, disinfecting coops and incinerating dead birds hasn't prevented the disease from becoming endemic in the country that has 1.3 billion poultry. The government hasn't raised sufficient public awareness of the dangers of the H5N1 virus and can't properly fund its avian flu programs, particularly those aimed at controlling the virus in poultry, Krisnamurti said.

Source: <http://www.bloomberg.com/apps/news?pid=10000101&sid=aCArWAVGRzmg&refer=japan>

29. *June 21, Reuters* — Up to 53 million people carry resistant staph, research says. Up to 53 million people worldwide could be carrying Methicillin-resistant Staphylococcus Aureus (MRSA), scientists said on Wednesday, June 21. Scientists estimate that around two billion people, some 25–30 percent of the world's population, have a form of the bacteria Staphylococcus Aureus. "Of those ... conservative estimates based on either Dutch or U.S. prevalence figures, would predict that between two million and 53 million carry MRSA," said Hajo Grundmann, one of the researchers. He said the large discrepancy between the higher and

lower ends of that estimate was due to differences in the way surveys were conducted. Grundmann, from the National Institute for Public Health and the Environment in Bilthoven, the Netherlands, said that "fitter" strains of MRSA had evolved which were even more resistant to treatment.

MRSA information: http://www.cdc.gov/ncidod/diseases/submenus/sub_mrsa.htm

Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006-06-21T122042Z_01_L20860350_RTRUKOC_0_US-MRSA.xml&archived=False

[[Return to top](#)]

Government Sector

30. *June 21, Chicago Tribune* — **White powder triggers federal building evacuation.** About 100 people were evacuated Monday, June 19, from a Chicago federal building that houses Citizenship and Immigration Services offices after a suspicious white substance, which turned out to be powdered sugar, was found in a mailroom. Fire Department hazardous materials crews quickly determined that the substance was powdered sugar, the department said. The building houses the Chicago district office of the U.S. Bureau of Citizenship and Immigration Services, according to the agency's Website.

Source: <http://www.chicagotribune.com/news/local/chicago/chi-0606200244jun20.1.4621946.story?ctrack=1&cset=true>

[[Return to top](#)]

Emergency Services Sector

31. *June 21, Virginian-Pilot* — **Regionwide evacuation drill conducted in Virginia.** As a mock hurricane advanced on Hampton Roads, VA, Tuesday, June 20, highways clogged with vehicles and an evacuation slowed to a crawl. The situation was shaping up as the drill's planners expected: horribly. James E. Mock, operations engineer at the Virginia Department of Transportation's (VDOT) Smart Traffic Center in Virginia Beach, was one of the organizers of Tuesday's first regionwide evacuation drill. A key to the exercise was turning all lanes of Interstate 64 into a westbound-only escape route. Just to patrol the 80 miles of I-64 that would be turned into a westbound-only route, VDOT says, roughly 500 personnel from VDOT, the State Police and the Virginia National Guard would be needed at ramps and crossover lanes. The drill organizers wanted to see how long it would take that many people to reach their assigned posts. "The results show that our test went very well," said Stephany D. Hanshaw, the Smart Traffic Center manager. He said all crews arrived at their spots within an hour of getting notice, with the equipment needed to divert traffic.

Source: <http://home.hamptonroads.com/stories/story.cfm?story=106399&ran=234691>

32. *June 20, Government Health IT* — **OASIS adopts info sharing standard for emergency responders.** Emergency responders in the field now have a data-sharing standard that provides role-based information sharing in a crisis. The Organization for the Advancement of Structured Information Standards (OASIS), a nonprofit, international consortium, has approved the

Emergency Data Exchange Language Distribution Element (EDXL–DE) Version 1.0 as an OASIS standard. EDXL–DE facilitates emergency information sharing and data exchange across local, regional, tribal, national and international organizations in the public and private sectors, OASIS officials said. The Department of Homeland Security (DHS) has collaborated since 2004 with private–sector members of the Emergency Interoperability Consortium (EIC), a public/private partnership, to create EDXL, OASIS officials said. DHS and the EIC created the requirement for the standard and OASIS developed the actual standard, according to Elysa Jones, chairwoman of the OASIS Emergency Management Technical Committee.

Source: <http://govhealthit.com/article94971-06-20-06-Web>

- 33. *June 01, Congressional Research Service* — CRS reports history and organizational structure of federal emergency management.** The Congressional Research Service (CRS) has released the report, "Federal Emergency Management and Homeland Security Organization: Historical Developments and Legislative Options." The report provides background information on the establishment and evolution of federal emergency management organizational arrangements since the end of World War II and briefly summarizes the legislative proposals put forth.

Source: <http://www.fas.org/sgp/crs/homesec/RL33369.pdf>

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

- 34. *June 20, eWeek* — Unpatched iTunes, Skype, Firefox inviting malware targets.** Unpatched versions of some of the most popular software applications present a bigger threat to enterprise networks than malicious software, according to a warning from Bit9, an endpoint security vendor. Bit9 on Tuesday, June 20, released a list of 15 widely deployed applications with critical vulnerabilities that go unnoticed in enterprise IT organizations and urged businesses to clamp down on the use of out–of–date software. The Bit9 list includes versions of several mainstream products — Mozilla Firefox, Apple's iTunes and QuickTime, Skype, Adobe Acrobat Reader and Sun Java Runtime Environment — that contain critical, code–execution vulnerabilities. The company said the list is limited to applications that are well known in the consumer space and are frequently downloaded by employees, often without the approval of IT departments.

Bit9's list: <http://www.bit9.com/docs/15VulnerableApps.pdf>

Source: <http://www.eweek.com/article2/0.1895.1979388.00.asp>

- 35. *June 20, Tech Web* — AT&T study finds companies aren't prepared for disasters.** AT&T Inc.'s fifth–annual Business Continuity Survey released Tuesday, June 20, which polled about 1,000 CIOs and IT executives at U.S. companies with more than \$10 million in annual revenue, reveals that 28 percent do not have adequate plans in place to cope with natural or other disasters. Nearly 30 percent of executives who participated in the survey said their company has suffered from a disaster. Eighty–one percent of executives said cyber security is part of their overall business plan for interruptions in 2006, up from 75 percent in 2005. Eight out of 10 companies have revised plans in the past 12 months, including 48 percent that say they've been updated in the past six months. Of those companies with plans in place, 40 percent say they have not tested their plan in the past year.

AT&T's study: http://www.sbc.com/Common/files/pdf/biz_cont_full_report.pdf
Source: <http://www.techweb.com/wire/security/189501126;jsessionid=MDZTKTAGQVT5UQSNDLPCKH0CJUNN2JVN>

36. *June 20, CNET News* — **'Critical' Microsoft fix breaks some Internet connections.** One of the dozen security updates Microsoft released last week with security bulletin MS06-025 is causing network connection trouble for some users, the company said. Problems occur only with dial-up connections that use a terminal window, or dial-up scripting, Microsoft said in an article on its support Website published late Monday, June 19. Microsoft is working on a revised security patch to address the issue. Meanwhile, the company recommends that people who need to use dial-up scripting or terminal window features do not install the security update.

Microsoft-released article on this issue: <http://support.microsoft.com/kb/911280>

Source: http://news.com.com/Critical+Microsoft+fix+breaks+some+Net+connections/2100-1002_3-6086130.html?tag=nefd.top

37. *June 20, Agence France-Presse* — **Future mobile telephone growth to come from poorer countries.** Future growth in the mobile telephone business will come from developing economies whose less than affluent consumers cannot be overlooked, industry players said. Income levels of consumers in the world's poorer nations may not come anywhere near their wealthy counterparts but they offer far better growth prospects for the sector as a whole, telecommunications executives said at CommunicAsia2006, a major four-day exhibition and associated conferences which opened in Singapore Tuesday, June 20. Asian countries that fall into the high growth category include Pakistan, Indonesia, China, India and the Philippines, where rural areas remain largely untapped, industry players said.

Source: http://news.yahoo.com/s/afp/20060620/tc_afp/asiatelecommobile:ylt=AgRhFSDd_d8EH6mKYCgU5NojtBAF;ylu=X3oDMTA0cDJlYmhvBHNlYwM-

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is aware of active exploitation of a new vulnerability in Microsoft Excel. Successful exploitation could allow an attacker to execute arbitrary code with the privileges of the user running Excel. For more information please review the following:

Technical Cyber Security Alert: TA06-167A

<http://www.us-cert.gov/cas/techalerts/TA06-167A.html>

Vulnerability Note: VU#802324 <http://www.kb.cert.org/vuls/id/802324>

We are continuing to investigate this vulnerability. US-CERT recommends the following actions to help mitigate the security risks:

Install anti-virus software, and keep its virus signature files up to date.

Limit user privileges to no administrator rights.

Save and scan any attachments before opening them.

Review the workarounds described in Microsoft Security Advisory 921365:

<http://www.microsoft.com/technet/security/advisory/921365.mspx>

US-CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04-010 for more information on working with email attachments: <http://www.us-cert.gov/cas/tips/ST04-010.html>

FDIC Phishing Scam

US-CERT continues to receive reports of phishing scams that target online users. Recently, the phishing scam targeted the customers of Federal Deposit Insurance Company (FDIC) insured institutions.

Customers of FDIC institutions received a spoofed email message, which claims that their account is in violation of the Patriot Act, and that FDIC insurance has been removed from their account until their identity can be verified. The message provides a link to a malicious web site which prompts users to enter their customer account and identification information.

If you were affected by the FDIC phishing scam, please refer to the FDIC Consumer Alert for assistance: <http://www.fdic.gov/consumers/consumer/alerts/phishing.html>

US-CERT confirms that the federal agencies including Department of Homeland Security (DHS) mentioned in the fraudulent email have not sent out an email that requests customer account or identification information.

US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT:

http://www.us-cert.gov/nav/report_phishing.html

Non-federal agencies and other users should report phishing incidents to OnGuard Online, a consortium of Federal Agencies: <http://onguardonline.gov/phishing.html>

Additionally, users are encouraged to take the following measures to prevent phishing attacks from occurring:

Do not follow unsolicited web links received in email messages.

Contact your financial institution and file a complaint with the Federal Trade Commission (FTC) immediately if you believe your account or financial information has been compromised.

[https://rn.ftc.gov/pls/dod/widtpubl\\$.startup?Z_ORG_CODE=PU03](https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03)

Review FTC's web site on how to protect yourself from identity theft:

<http://www.consumer.gov/idtheft/>

Review the OnGuard Online practical tips to guard against Internet fraud, secure your computer, and protect your personal information:

<http://onguardonline.gov/phishing.html>

Refer to the US-CERT Cyber Security Tip on Avoiding Social Engineering and Phishing Attacks: <http://www.us-cert.gov/cas/tips/ST04-014.html>

Refer to the CERT Coordination Center document on understanding Spoofed/Forged Email: http://www.cert.org/tech_tips/email_spoofing.html

PHISHING SCAMS

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

http://www.us-cert.gov/nav/report_phishing.html

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 4049 (----), 6881 (bittorrent), 3795 (----), 38566 (----), 445 (microsoft-ds), 25 (smtp), 32790 (----), 24232 (----), 113 (auth) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

General Sector

38. *June 21, Fox News* — Firefighters fighting 1,770-acre Arizona wildfire. Firefighters early Wednesday, June 21, battled a 1,770-acre wildfire that forced hundreds of people to evacuate and threatened a highway and homes at the bottom of Arizona's scenic Oak Creek Canyon. Only five percent contained, the blaze — started Sunday, June 18, as a transient's campfire — was within 200 yards of the highway in some stretches along the canyon bottom, authorities said. At risk in Arizona are hundreds of homes, lodges, picnic areas, campgrounds, and structures in the area of Slide Rock State Park, a popular recreation spot that draws hundreds of thousands of visitors a year. Crews also battled wildfires in Colorado, New Mexico, and California.

Source: <http://www.foxnews.com/story/0.2933.200382.00.html>

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.